Sorbonne Université
Théorie des Nombres 2 (MU4MA034)
Mars–Mai 2021.

Séance 1, 8 mars 2021

Notations et conventions.

- Pour $r \in \mathbb{Q}$ positif, le symbole $\sqrt{r}$ est le réel usuel.
- Le nombre algébrique α a "degré" n quand $[\mathbb{Q}(\alpha) : \mathbb{Q}] = n$.
- Pour chaque nombre algébrique α, on désigne par $\Pi_\alpha \in \mathbb{Q}[X]$ son polynôme minimal.
- Si K un corps de nombres de degré n, l'ensemble de plongements de K dans $\mathbb{C}$ est noté $\Sigma(K)$. Si $\alpha \in K$ est donné, les conjugués de α sont les complexes ayant la forme $\sigma(\alpha)$ pour $\sigma \in \Sigma(K)$. La K-norme $\mathrm{N}_K(\alpha)$ est $\prod_{\sigma\in\Sigma(K)} \sigma(\alpha)$ et la K-trace $\mathrm{Tr}_K(\alpha)$ est $\sum_{\sigma\in\Sigma(K)} \sigma(\alpha)$. (Une notation plus précise et plus encombrante serait $\mathrm{N}_{K/\mathbb{Q}}(\alpha)$ et $\mathrm{Tr}_{K/\mathbb{Q}}(\alpha)$.)
- Pour $n \geqslant 1$, on désigne par μ_n, respectivement μ'_n, l'ensemble des racines n-èmes, respectivement n-èmes et primitives, de l'unité dans $\mathbb{C}$.
- Le n-ème polynôme cyclotomique $\prod_{\zeta\in\mu'_n}(X - \zeta)$ sera désigné par Φ_n.

Cyclotomie

Exercice 1. On étudie des propriétés basiques des corps cyclotomiques.

1/ Soient m, n des entiers strictement positifs. Montrer que si $\mathrm{pgcd}(m, n) = 1$, alors $\mathbb{Q}(\mu_m, \mu_n) = \mathbb{Q}(\mu_{mn})$. Indication : On pourra considérer le morphisme $f : \mu_m \times \mu_n \to \mu_{mn}$ définit par $(z, w) \mapsto zw$.

Correction. On note que f est un morphisme de groupes : $f(z, w)\cdot f(z', w') = zz'ww' = f(zz', ww')$. Puis, si $zw = 1$ alors $z^n = 1$, et comme l'ordre de $z \in \mu_m$ doit diviser m, ceci nous montre que $z = 1$. Donc, f est injectif et surjectif, d'où f est un isomorphisme. □

2/ Soit p un nombre premier *impair*. En utilisant que $\Phi_p(1) = p$, montrer que $p^* := (-1)^{(p-1)/2}p$ est un carré en $\mathbb{Q}(\mu_p)$. En déduire que pour chaque premier impair p, le corps $\mathbb{Q}(\mu_{4p})$ contient $\sqrt{p}$ et $\mathrm{i}\sqrt{p}$.

Correction. Soit ζ une racine primitive p-ème de l'unité. On sait que $p = \Phi_p(1) =$

$\prod_{j=1}^{p-1}(1-\zeta^j)$. Ceci peut être récrit comme

$$p = \prod_{j=1}^{(p-1)/2} (1-\zeta^j)(1-\zeta^{p-j}).$$

Or, $1-\zeta^{p-j} = -\zeta^{-j}(1-\zeta^j)$. D'où

$$p = (-1)^{\frac{p-1}{2}} \zeta^{-1-2-\cdots-\frac{p-2}{2}} \prod_{j=1}^{\frac{p-1}{2}} (1-\zeta^j)^2.$$

Or, comme une puissance ζ^r est toujours un carré car $(-)^2 : \mu_p \to \mu_p$ est un isomorphisme, on déduit que $(-1)^{\frac{p-1}{2}} p$ est un carré. Si $p \equiv 1 \mod 4$, alors $\sqrt{p} \in \mathbb{Q}(\mu_p)$ et $\mathrm{i}\sqrt{p} \in \mathbb{Q}(\mu_{4p})$. Si $p \equiv 3 \mod 4$ alors $\mathrm{i}\sqrt{p} \in \mathbb{Q}(\mu_p)$ et $\sqrt{p} \in \mathbb{Q}(\mu_{4p})$. □

3/ Déterminer un corps cyclotomique $\mathbb{Q}(\mu_n)$ contenant $\sqrt{2}$ et $\mathrm{i}\sqrt{2}$.

Correction. Il est clair que $\mathbb{Q}(\mu_8)$ suffit : en effet, $2e^{\mathrm{i}\pi/4} = \sqrt{2} + \mathrm{i}\sqrt{2}$ et $2e^{-\mathrm{i}\pi/4} = \sqrt{2} - \mathrm{i}\sqrt{2}$. □

4/ En déduire que chaque corps quadratique de nombres est contenu dans un corps cyclotomique.

Correction. Soit $d > 0$ un entier sans facteur carré. On l'écrit $d = p_1 \cdots p_r$ où $0 < p_1 < \cdots < p_r$ sont premiers. Si $p_1 = 2$, on sait que $\sqrt{p_1}$ et $\mathrm{i}\sqrt{p_1}$ appartiennent à $\mathbb{Q}(\mu_8)$. Ensuite, $\sqrt{p_j}$ et $\mathrm{i}\sqrt{p_j}$ appartiennent à $\mathbb{Q}(\mu_{4p_j})$. Donc, $\mathrm{i}\sqrt{d}$ et $\sqrt{d}$ appartiennent à $\mathbb{Q}(\mu_{4d})$. □

Exercice 2 (Les polynômes cyclotomiques)**.** Soit $n > 1$. Dans la suite on étudie

$$\Phi_n(X) = \prod_{\zeta \in \mu_n'} (X - \zeta) \in \overline{\mathbb{Q}}[X],$$

le n-ème polynôme cyclotomique.

(1) Montrer que[1] $\mu_n = \bigsqcup_{d|n} \mu_d'$, et utiliser cette équation pour déduire $X^n - 1 = \prod_{d|n} \Phi_d$.

Correction. Par définition, une racine primitive n-ème de l'unité est un élément de $\mathbb{C}^*$ d'ordre n. Or, soit $z \in \mu_n$ un élément d'ordre d. Il suit que $z \in \mu_d'$ et la formule

1. On rappelle que $\bigsqcup$ note la réunion disjointe.

$\mu\!\!\mu_n = \coprod_{d|n} \mu\!\!\mu'_d$ en découle. Puis,

$$\begin{aligned} X^n - 1 &= \prod_{\zeta \in \mu\!\!\mu_n} (X - \zeta) \\ &= \prod_{d|n} \prod_{z \in \mu\!\!\mu'_d} (X - \zeta) \\ &= \prod_{d|n} \Phi_d(X). \end{aligned}$$

□

(2) En déduire que $\Phi_n \in \mathbb{Z}[X]$. (Indication : La division Euclidienne "fonctionne" sur $\mathbb{Z}[X]$ tant qu'on divise par des polynômes unitaires.)

Correction. Pour montrer que $\Phi_n \in \mathbb{Z}[X]$, on fait une récurrence. Soit $F = \prod_{\substack{d<n \\ d|n}} \Phi_d(X)$, qu'on suppose appartenir à $\mathbb{Z}[X]$; c'est un polynôme unitaire en plus. Soit $X^n - 1 = F(X)Q(X) + R(X)$ la division Euclidienne, avec $Q, R \in \mathbb{Z}[X]$. Par unicité, cette formule est vraie dans $\mathbb{C}[X]$. Mais on sait que, dans $\mathbb{C}[X]$, la division euclidienne est

$$X^n - 1 = \Phi_n(X) \cdot F.$$

Par unicité, $Q = \Phi_n$ et $R = 0$. □

(3) Soit p premier. Rappeler la formule $\Phi_p = X^{p-1} + \cdots + 1$.

Correction. Les racines de $X^p - 1$ sont $\mu\!\!\mu'_p \cup \{1\}$. Donc, $X^p - 1 = \Phi_p(X) \cdot (X - 1)$, et la formule suit. □

(4) Pouvez-vous calculer explicitement Φ_{p^m}, où p est premier ? Quel est le lien entre ce dernier et Φ_p ?

Correction. On commence avec Φ_{p^2}. Or, $X^{p^2} - 1 = \Phi_{p^2}\Phi_p\Phi_1$. Or, mais $X^p - 1 = \Phi_p\Phi_1$ et donc $\Phi_{p^2} = \dfrac{X^{p^2} - 1}{X^p - 1}$. En général :

$$\Phi_{p^m} = \frac{X^{p^m} - 1}{X^{p^{m-1}} - 1} = \Phi_p(X^{p^{m-1}}).$$

□

(5) Calculer explicitement Φ_6 et Φ_{12}.

Correction. On sait que $\Phi_1 = X - 1$, $\Phi_2 = X + 1$ et $\Phi_3 = X^2 + X + 1$. Donc, $\Phi_6 = \dfrac{X^6 - 1}{(X^2 - 1)(X^2 + X + 1)} = X^2 - X + 1$. Ensuite, $\Phi_{12} = X^4 - X^2 + 1$. □

Exercice 3 (Une preuve "euclidienne")**.** Soit $n \geqslant 1$ un entier. On souhaite utiliser Φ_n pour donner une preuve "euclidienne" de l'existence d'une infinité de premiers $\equiv 1 \mod n$. (Euclidienne, car en faisant la preuve avec $n = 1$ on arrive à la preuve célèbre d'Euclide sur l'existence d'un nombre infini de premiers.)

1/ Montrer que le coefficient *constant* de Φ_n est toujours ± 1. Utiliser ce fait pour prouver que $\mathrm{pgcd}(\alpha, \Phi_n(\alpha)) = 1$ pour tout entier non-nul α.

Correction. On note que

$$-1 = \prod_{d|n} \Phi_d(0).$$

De ce fait, $\Phi_n(0)$ divise -1 et donc $\Phi_n(0) = \pm 1$. Ensuite, on note que $\Phi_n(\alpha) \equiv \pm 1 \mod \alpha$ et si $d|\Phi_n(\alpha)$ ainsi que α, alors d divise ± 1. □

2/ Soit α un entier et p un facteur premier de $\Phi_n(\alpha)$. On suppose de plus que p ne divise pas n. Montrer que l'ordre de l'image $\tilde{\alpha}$ de α dans $\mathbb{F}_p^\times$ est n. Indication : Utiliser que $X^n - 1 \in \mathbb{F}_p[X]$ n'a que de racines simples et $X^n - 1 = \Phi_n \cdot F$, avec $F = \prod_{\substack{d|n \\ d<n}} \Phi_d$.

Correction. On sait que $\alpha^n - 1 = \Phi_n(\alpha)F(\alpha)$ avec $F = \prod_{\substack{d|n \\ d<n}} \Phi_d$ et par conséquent $\tilde{\alpha}^n - 1 \equiv 0 \mod p$. Soit $k = \mathrm{ord}(\tilde{\alpha})$; on en tire que $k|n$.
Comme $\alpha^k \equiv 1 \mod p$ et $\alpha^k - 1 = \prod_{d|k} \Phi_d(\alpha)$, on déduit que $\Phi_\ell(\alpha) \equiv 0 \mod p$ pour un certain diviseur ℓ de k. Donc $(X - \tilde{\alpha})^2$ divise $\tilde{\Phi}_n\tilde{\Phi}_\ell \in \mathbb{F}_p[X]$.
Si $k < n$, alors $\ell < n$ et $\Phi_n\Phi_\ell | X^n - 1$, d'où $(X - \tilde{\alpha})^2 | X^n - 1$ en $\mathbb{Z}[X]$. Ceci est impossible, car $X^n - 1$ n'a que des racines simples.

□

3/ Montrer qu'il existe un nombre infini de premiers $\equiv 1 \mod n$. Indication : Si $p_1, \ldots, p_r$ sont premiers $\equiv 1 \mod n$, on considère $\Phi_n(gnp_1 \cdots p_n)$ pour $g \to +\infty$.

Correction. Soit $g \in \mathbb{N}$ tel que $\Phi_n(gnp_1 \cdots p_r) > 1$. Soit p un facteur premier de $\Phi_n(gnp_1 \cdots p_r)$. Alors $gnp_1 \cdots p_r \not\equiv 0 \mod p$ d'après (1). En particulier, p ne divise pas n. On peut appliquer (2) : l'orde de $gnp_1 \cdots p_r$ est n dans $\mathbb{F}_p^*$ et donc $n|p-1$ par le théorème de Lagrange. □

Exercice 4 (Polynômes cyclotomiques : irréductibilité)**.** On fixe $\zeta \in \mu_n'$, p un premier *qui ne divise pas* n et on écrit $\xi = \zeta^p$. On montrera que Φ_n est irréductible en montrant d'abord que $\Pi_\xi = \Pi_\zeta$.

1/ Les polynômes Π_ζ et Π_ξ de $\mathbb{Q}[X]$ appartiennent en fait à $\mathbb{Z}[X]$: Justifier.

Correction. A été vu en cours : suit aussi du fait que les coefficients du polynôme minimal sont des entiers algébriques dans $\mathbb{Q}$, donc des entiers. □

2/ Il existe $F \in \mathbb{Z}[X]$ tel que $\Pi_\zeta(X)F(X) = \Pi_\xi(X^p)$: Justifier.

Correction. Puisque $\Pi_\xi(\zeta^p) = 0$, il existe $F \in \mathbb{Q}[X]$ tel que $\Pi_\zeta(X)F(X) = \Pi_\xi(X^p)$. Or, comme la division euclidienne "fonctionne" en $\mathbb{Z}[X]$ pour des polynômes unitaires, on voit que $F \in \mathbb{Z}[X]$. □

3/ Utiliser la question précédente pour montrer que les images dans $\mathbb{F}_p[X]$ de Π_ζ et Π_ξ ont un diviseur commun.

Correction. On note l'image dans $\mathbb{F}_p[X]$ par un tilde. Or, on sait que $\tilde{\Pi}_\xi(X^p) = \tilde{\Pi}_\zeta(X)\tilde{F}(X)$. Mais $\tilde{\Pi}_\xi(X^p) = (\tilde{\Pi}_\xi(X))^p$. Donc, $\tilde{\Pi}_\xi^p = \tilde{\Pi}_\zeta\tilde{F}$, et l'affirmation suit. □

4/ Montrer que $\Pi_\zeta = \Pi_\xi$. Indication : Si $\Pi_\zeta \neq \Pi_\xi$, alors $X^n - 1 \in \mathbb{F}_p[X]$ est divisible par un carré.

Correction. On a $X^n - 1 = \Pi_\zeta\Pi_\xi \cdot G$ avec $G \in \mathbb{Z}[X]$. Donc, $X^n - 1 = \tilde{\Pi}_\zeta\tilde{\Pi}_\xi \cdot \tilde{G}$ et $X^n - 1$ possède un facteur avec multiplicité. Ceci est faux. □

5/ Monter que $\Phi_n = \Pi_\zeta$ et en déduire que Φ_n est irréductible.

Correction. Soit $\omega \in \boldsymbol{\mu}_n'$. Comme $\boldsymbol{\mu}_n$ est cyclique, on peut écrire $\omega = \zeta^k$. Puisque ω a ordre n en $\boldsymbol{\mu}_n$, on sait que $k = p_1 \cdots p_r$ avec p_i un premier qui ne divise pas n. Donc,

$$\Pi_\zeta = \Pi_{\zeta^{p_1}} = \Pi_{\zeta^{p_1 p_2}} = \cdots = \Pi_\omega.$$

Par conséquent, Π_ζ s'annule sur $\boldsymbol{\mu}_n'$ et donc $\deg \Phi_n \geqslant \deg \Pi_\zeta$. Comme $\Pi_\zeta | \Phi_n$, on déduit que $\Pi_\zeta = \Phi_n$. □